Расчёт надёжности на этапе системного анализа

Проектируй надёжность заранее

Живых Арсений Анатольевич

24-25.09.2024

Арсений Живых

Старший системный аналитик

Магистратура
НИУ ВШЭ
с отличием

Продукт Ревизор
(внутренний
антифрод)

t.me/ArsZhivyh

О важности надёжности

Важность надёжности информационных систем

Надёжность

Оказание услуг клиентам

Клиентов обычно раздражает если банковское приложение не работает

Выполнение SLA перед соседями

Одна ненадёжная система может создать трудности всей организации

Ночные дежурства

На каждый произошедший сбой нужно потратить силы и время

Когда и как обычно задумываются о надёжности

На собственном опыте

Проектирование

- Распределение ресурсов
- Отказоустойчивые компоненты
- Безопасность
- Резервное копирование данных

Тестирование

- Нагрузочное
- Регрессионное
- Интеграционное

Эксплуатация

- Дежурства
- Добавление ресурсов
- Мониторинг метрик
- Планирование релизов

Как оценить при проектировании

Теоретическое вступление о вероятности работы

Вероятность работы в момент времени – вероятность того, что запрос будет корректно обработан за установленный SLA

Теория

Для синхронных интеграций:

Доступность + время ответа < SLA

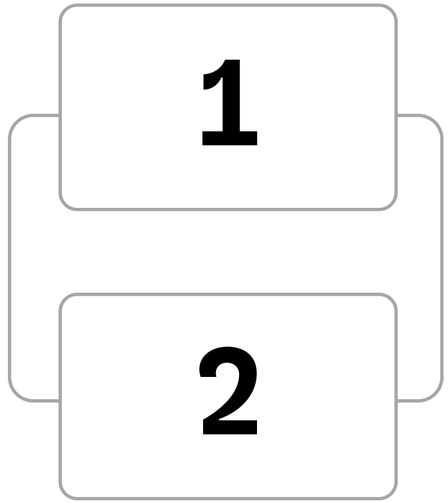
Для асинхронных интеграций:

Время обработки сообщения < SLA

Теоретическое вступление о надёжности

Надёжность – вероятность корректной работы процесса в момент времени

Теория



Вероятность бесперебойной работы

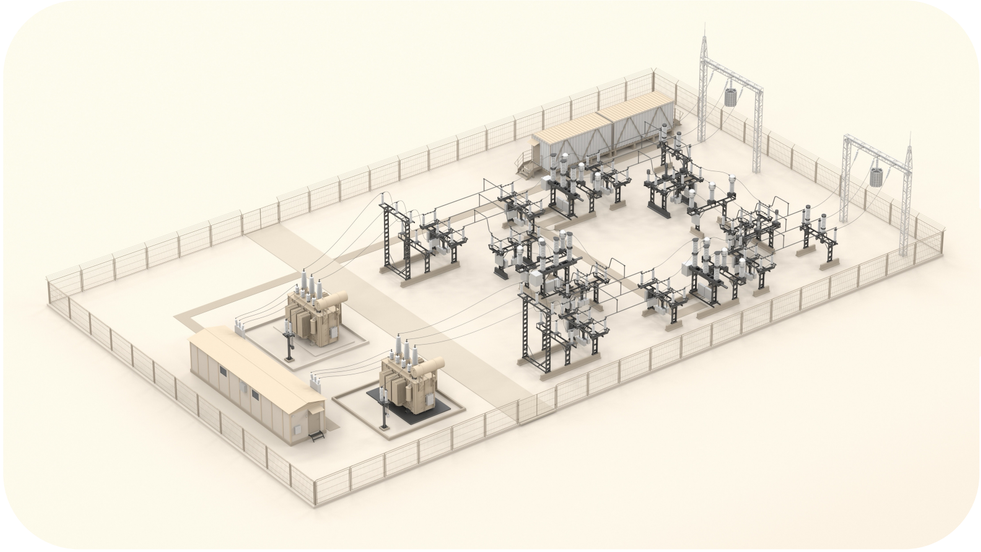
$$P_O = P_1 P_2$$

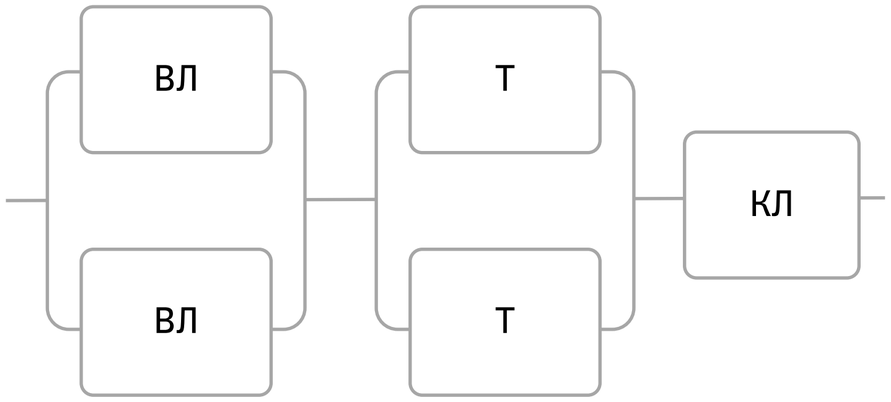
Вероятность отказа

$$Q_O = Q_1 Q_2 \rightarrow 1 - P_O = (1 - P_1)(1 - P_2)$$

$$P_o = P_1 + P_2 - P_1 P_2$$

Откуда появилась идея





ВЛ – воздушная линия

Т – трансформатор

КЛ – кабельная линия

На схеме 2 воздушные линии параллельно входят в два трансформатора и допустим, что дальше есть кабельная линия

$$P_o = (1-Q_{VL}^2)(1-Q_T^2)(1-Q_{KL}) =$$
$$(1-0.0002^2)(1-0.0005^2)0.9999 \approx 99.99\%$$

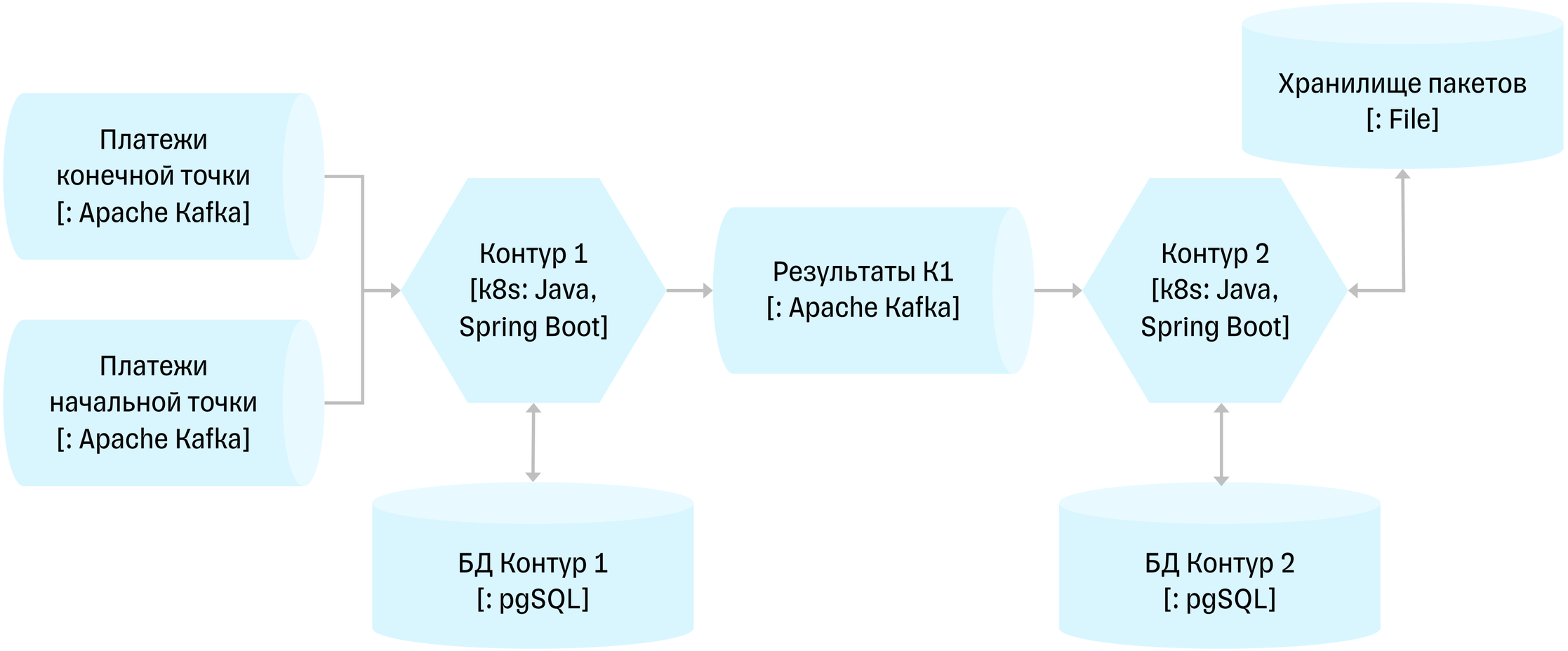
Оценка надёжности по архитектуре

Основная идея

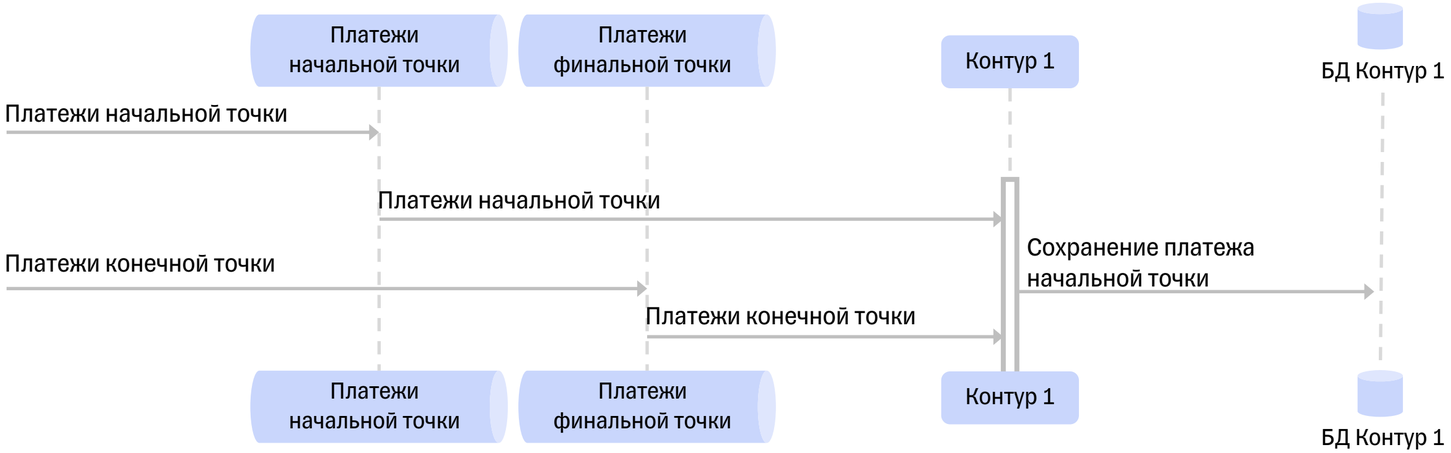
Вероятность отказа: $Q_o = 1 - (1 - Q_{ib})^2(1 - Q_{ip})^2(1 - Q_{balanc}^2)(1 - Q_{fraud}^n)$

Вероятность бесперебойной работы: $P_o = 1 - Q_0 = (1 - Q_{ib})^2(1 - Q_{ip})^2(1 - Q_{balanc}^2)(1 - Q_{fraud}^n)$

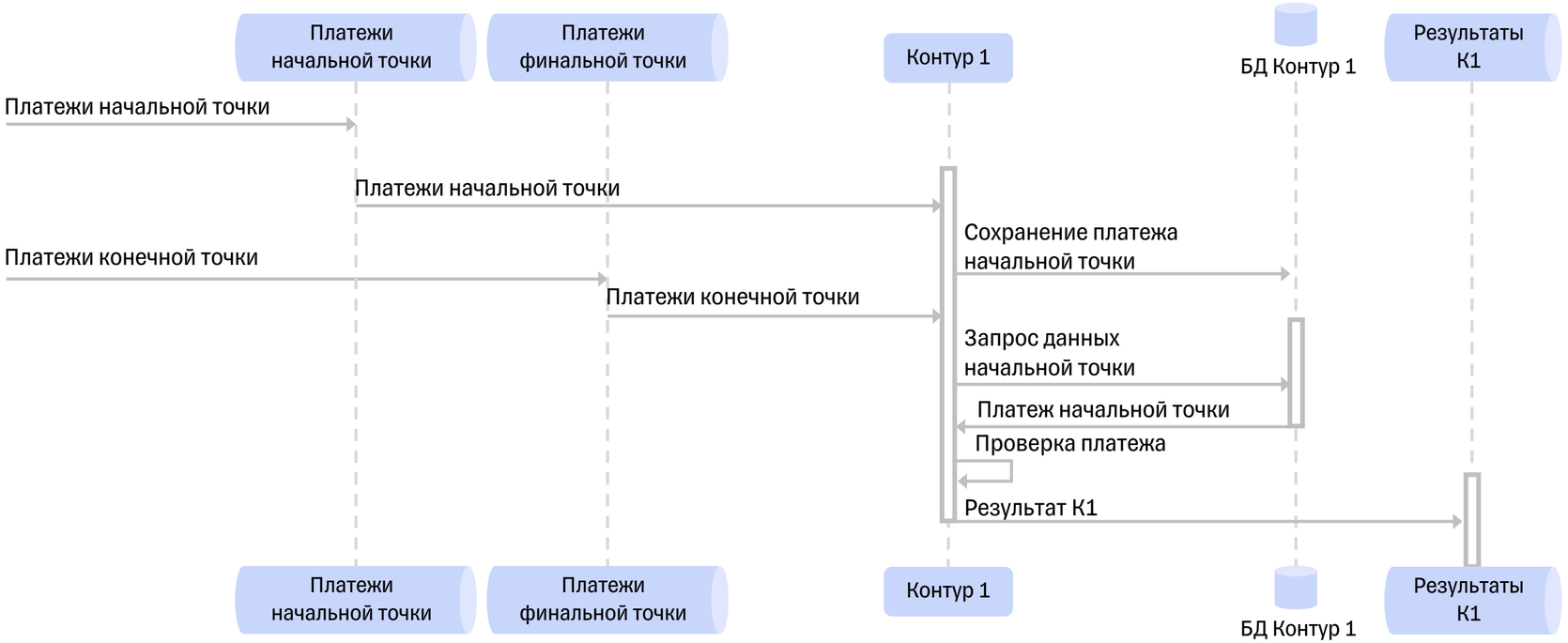
Пример: архитектура 2 контура



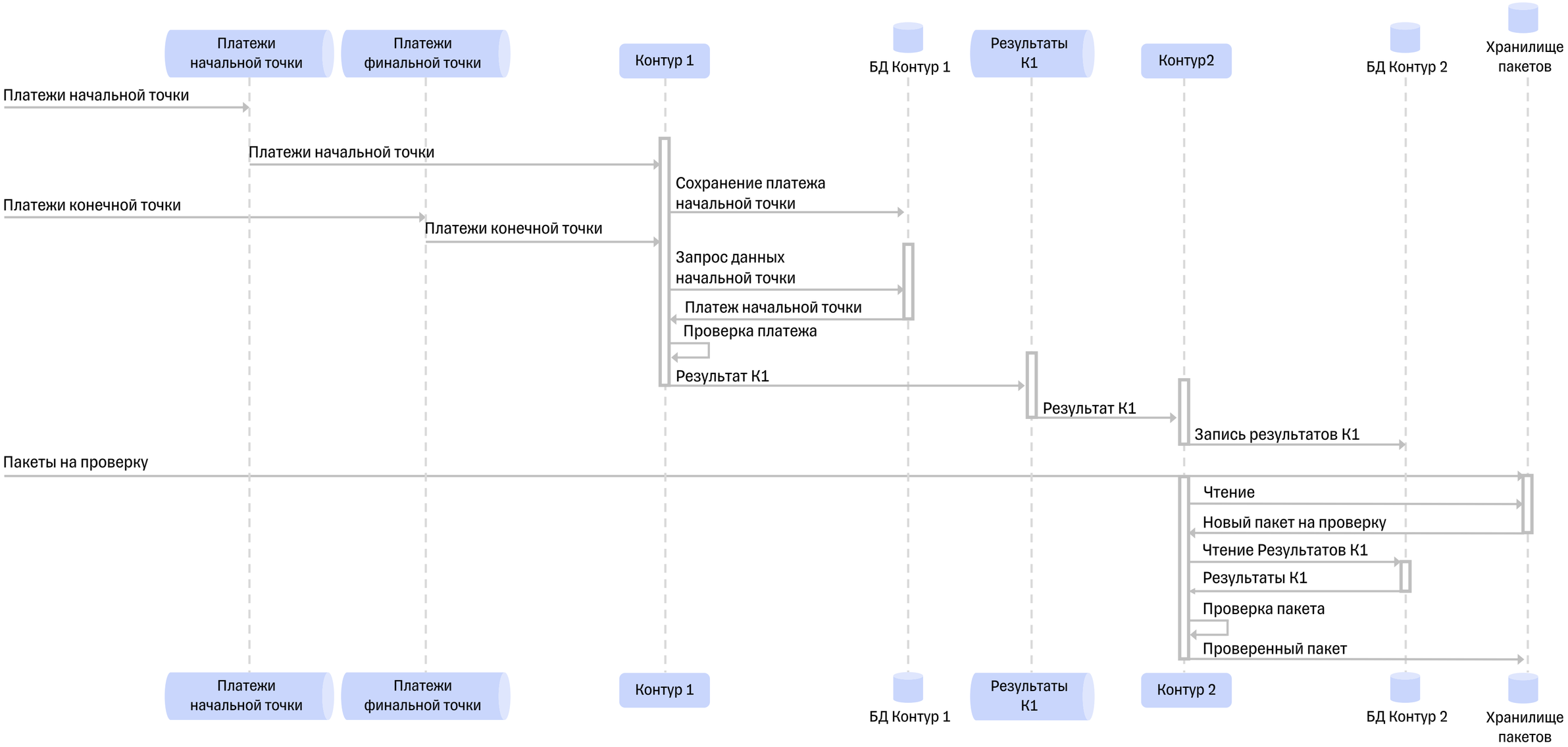
Пример: архитектура 2 контура



Пример: архитектура 2 контура



Пример: архитектура 2 контура



Формула архитектуры 2 контура

Вероятность бесперебойной работы: $P_O = P_{SP} P_P P_{K1}^2 P_{DB1}^2 P_{RK1} P_{K2}^2 P_{DB2}^2 P_{FTP}^2$

$$P_{K1} = 2P_c - P_c^2$$

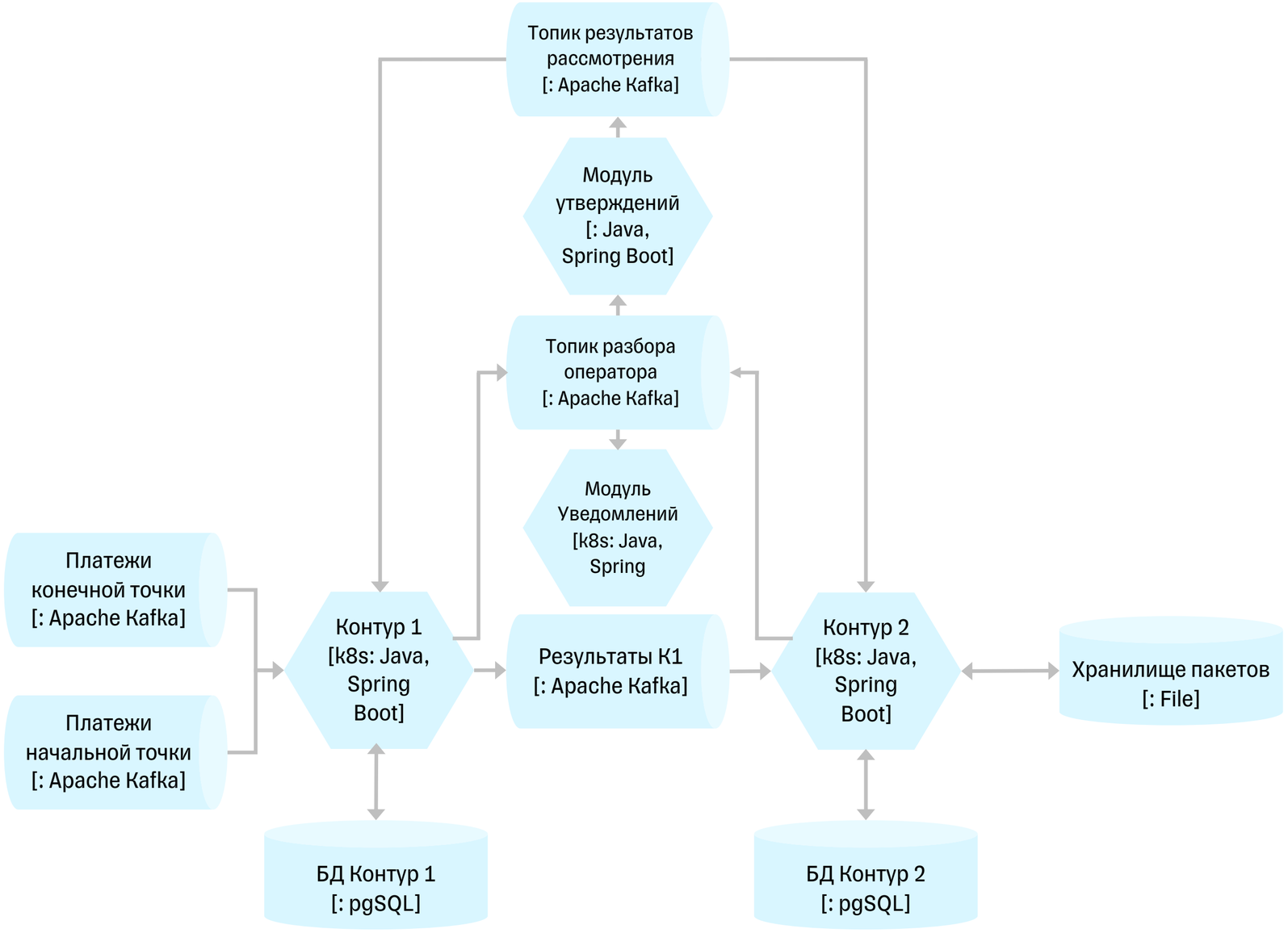
Из преобразования, что вероятность отказа К1 равна вероятности отказа двух ЦОДов, где он развёрнут

$$Q_{K1} = Q_c^2$$

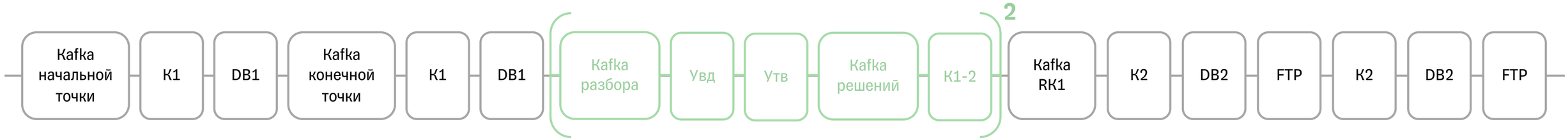
$$P_{K2} = 2P_c - P_c^2$$

Индекс	Расшифровка
SP	Топик платежей начальной точки
P	Топик платежей конечной точки
К1	Сервис Контура 1
DB1	БД Контура 1
RK1	Топик результатов контура 1
К2	Сервис Контура 2
DB2	БД Контура 2
FTP	Хранилище пакетов
C	Сервис в одном ЦОДе

Расширение системы



Формула архитектуры 2 контура+Оператор



Вероятность бесперебойной работы: $$P_O = P_{SP} P_P P_{K1}^2 P_{DB1}^2 P_{RK1} P_{K2}^2 P_{DB2}^2 P_{FTP}^2 \; P_{OP}$$

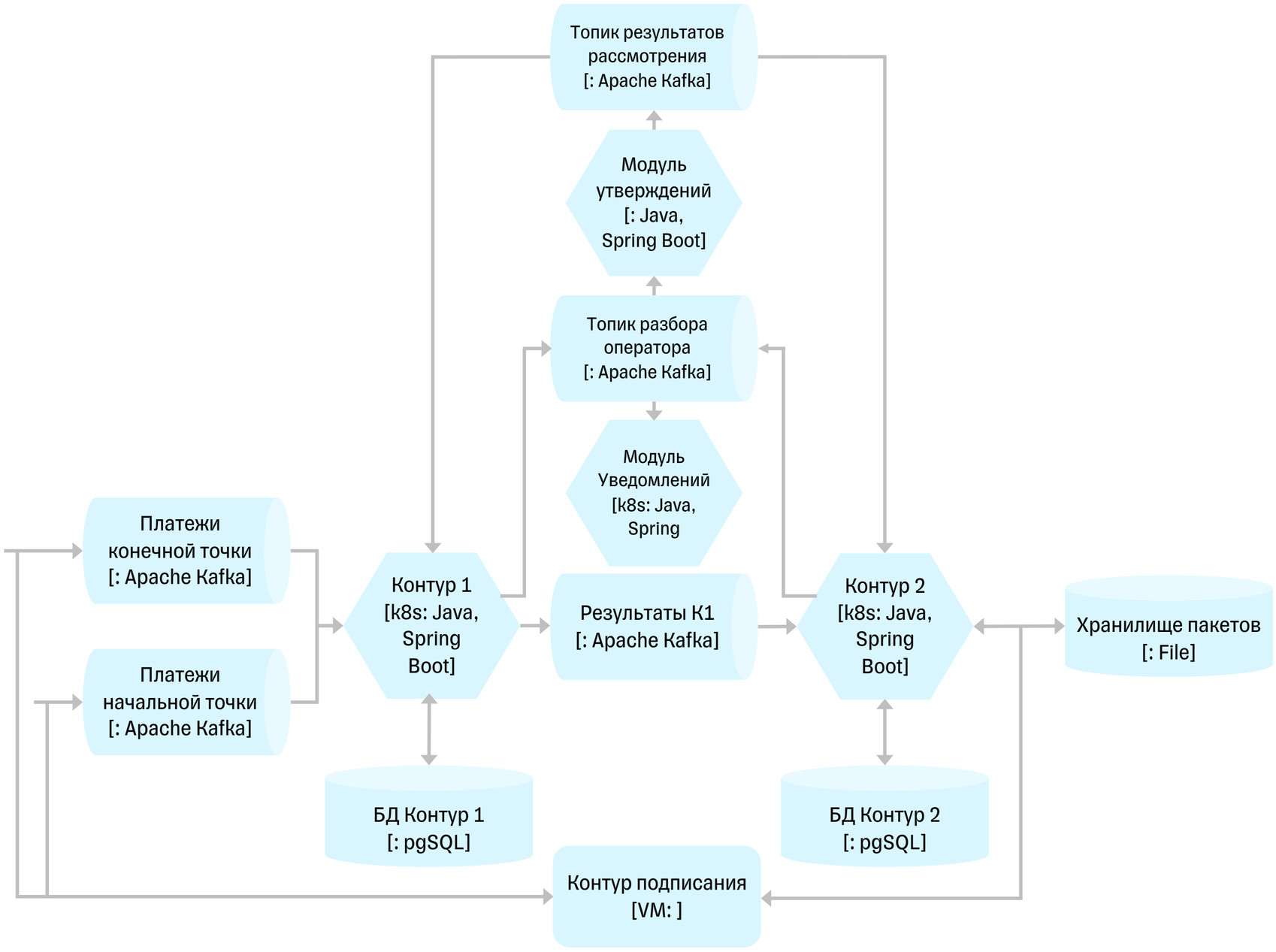
$$P_{OP} = (P_{RA} P_{YBD} P_{YTB} P_{RE} P_{K1})^2$$

Индекс	Расшифровка	Надёжность, %
RA	Топик платежей на разбор	99,95
YBD	Модуль уведомлений	99,8
YTB	Модуль утверждений	99,8
RE	Топик результатов разбора	99,95

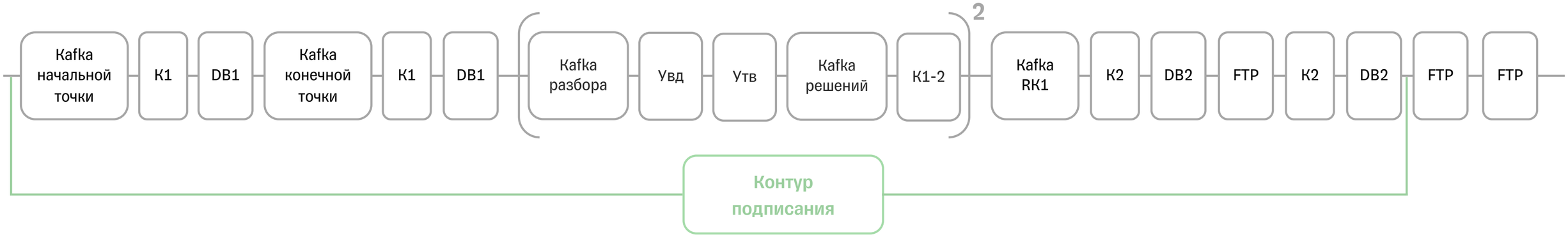
$$P_O \approx 0,9822 \cdot 0,99 \approx 0,973$$

Индекс	Расшифровка	Надёжность, %
SP	Топик платежей начальной точки	99,95
P	Топик платежей конечной точки	99,95
К1	Сервис Контура 1	99,8
DB1	БД Контура 1	99,8
RK1	Топик результатов контура 1	99,95
К2	Сервис Контура 2	99,8
DB2	БД Контура 2	99,8
FTP	Хранилище пакетов	99,95
С	Сервис в одном ЦОДе	99,6

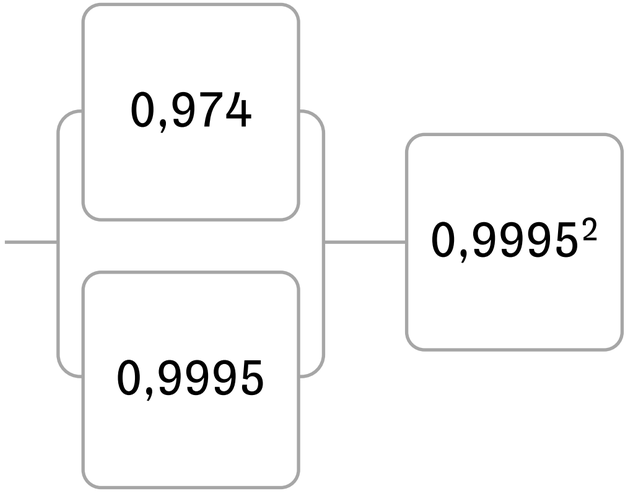
Повышение надёжности



Формула архитектуры Контур подписания



$$P_O = (0,974 + 0,9995 - 0,974 \cdot 0,9995)0,9995^2 \approx 99,9\%$$



99,96%

Реальная надёжность (сколько документов обработали за заданный SLA)

На каком уровне применять

На любом, где хватает данных для расчёта

На уровне сквозного процесса

Какие есть системы и связи между ними

На уровне системы или решения

Какие компоненты и как участвуют в процессе

На уровне одного сервиса

Из каких инфраструктурных составляющих состоит сервис и какая надёжность этой инфраструктуры

О требованиях

- Скорость выполнения одного конкретного шага
- Доступность сервиса

+ Отличия требуемой и реальной надёжности
+ Расчёт с точки зрения выполнения процесса за заданный SLA
+ Формулировать надёжность в привязке к SLA

Как можно применить у себя

Применение

Сформулировать процесс

В том числе перечень участвующих элементов

Собрать статистику надёжности элементов

Реальное выполнение SLA

Реальная доступность с учётом нагрузки

Структурная схема

Реальная доступность без нагрузки

Требуемая доступность

Выполнить вычисления

Что можно улучшить

Методика

Доработать методику

- Сбор статистики надёжности и классификация элементов архитектуры
- Найти наиболее подходящую нотацию

Решить проблемы

- Автоматизация расчёта
- Учёт нагрузки в расчёте
- Учёт надёжности сети

Выводы

Проектируй надёжность заранее

Системный подход к проектированию надёжности

При проектировании можно системно подходить к проектированию надёжности, а не только на личном опыте

Альтернативная ветка процесса значительно увеличивает надёжность

Для критичных систем имеет смысл создавать независимый альтернативный Flow

Т БАНК

Спасибо!